JOURNAL OF NUMBER THEORY **58**, 361–387 (1996)
ARTICLE NO. 0082

Über Arithmetische Assoziierte Ordnungen

W. BLEY*

Institut für Mathematik, Universität Augsburg, Universitätsstrasse 8, D-86159 Augsburg, Deutschland

UND

D. BURNS†

Mathematics Department, King's College London, Strand, London WC2R 2LS, England

Let p be an odd rational prime, and L/K a totally ramified finite abelian extension of p-adic fields. Let G denote the Galois group of L/K. For each ideal I of the valuation ring of L we study its "associated order" $End_{\mathbb{Q}_p[G]}(I)$ with respect to $\mathbb{Q}_p[G]$. This order is a natural operating ring for the ideal I, and is an important invariant of its $\mathbb{Z}_p[G]$-structure. We show that unless G is cyclic no such order can contain any idempotent of $\mathbb{Q}_p[G]$ which does not already lie in $\mathbb{Z}_p[G]$. This is a strong restriction on the possible structures of arithmetical associated orders. We also describe an algorithm for the explicit computation of associated orders which can in many cases be implemented effectively on a computer. In this way we are able to compute explicit examples of arithmetical associated orders which falsify a conjecture previously made by the second named author.

1. EINLEITUNG

Sei p eine rationale Primzahl. Für einen p-adischen Zahlkörper F bezeichne $\mathcal{O}_F$ den Ring der ganzen Zahlen in F, $\mathfrak{p}_F$ das maximale Ideal von $\mathcal{O}_F$ und e_F den Verzweigungsindex von $\mathcal{O}_F/\mathbb{Z}_p$. Sei L ein endlicher, abelscher Erweiterungskörper des p-adischen Zahlkörpers K, $G_{L/K}$ die zugehörige Galoisgruppe und $\{G_{L/K}^{(i)}\}_{i \geq -1}$, bzw. $\{G_{L/K,(i)}\}_{i \geq -1}$ die Verzweigungsgruppenreihe in oberer, bzw. unterer Numerierung. Es gilt $G_{L/K}^{(0)} = G_{L/K}^{(1)} \times C_{L/K}$, wobei $G_{L/K}^{(1)}$ die p-Sylowuntergruppe von $G_{L/K}^{(0)}$ und $C_{L/K}$ eine zyklische Untergruppe ist. Wir setzen $P_{L/K} = G_{L/K}^{(1)}$. Sei E ein Unterkörper

* E-mail: bley@uni-augsburg.de.
† E-mail: udah016@bay.cc.kcl.ac.uk.

0022-314X/96 $18.00

von K. Der Körper L ist ein freier $E[G_{L/K}]$-Modul vom Rang $[K:E]$. Ferner wirkt der ganzzahlige Gruppenring $\mathcal{O}_E[G_{L/K}]$ in natürlicher Weise auf jedes gebrochene $\mathcal{O}_L$-Ideal $\mathfrak{p}_L^k$, $k \in \mathbb{Z}$. Die $\mathcal{O}_E[G_{L/K}]$-Struktur jedes solchen Ideals ist jedoch höchst kompliziert. Sogar in dem sehr speziellen Fall, daß $\mathcal{O}_E[G_{L/K}]$ von endlichem Darstellungstyp ist, kennt man die Struktur von $\mathcal{O}_L$ als $\mathcal{O}_E[G_{L/K}]$-Modul nur teilweise (siehe [16]), und im allgemeinen Fall scheint ihre explizite Beschreibung ein kaum faßbares Problem darzustellen (siehe etwa [10]).

Für jedes Paar von Idealen $\mathfrak{p}_L^{k_1}$ und $\mathfrak{p}_L^{k_2}$ sei $\mathcal{A}(E[G_{L/K}]; k_1, k_2)$ der $\mathcal{O}_E[G_{L/K}]$-Modul der Elemente λ von $E[G_{L/K}]$, die der Bedingung $\lambda(\mathfrak{p}_L^{k_1}) \subseteq \mathfrak{p}_L^{k_2}$ genügen. Besonders interessant ist der Fall $k_1 = k_2$, wo $\mathcal{A}(E[G_{L/K}]; k_1, k_2)$ eine $\mathcal{O}_E$-Ordnung ist, die sogenannte *assoziierte Ordnung* von $\mathfrak{p}_L^{k_1}$ in Bezug auf $E[G_{L/K}]$. In diesem Fall setzen wir $\mathcal{A}(E[G_{L/K}]; k_1) := \mathcal{A}(E[G_{L/K}]; k_1, k_1)$. Explizite Beschreibungen von assoziierten Ordnungen sind deshalb von großem Interesse, weil sie die natürlichen Operatorenringe für gebrochene Ideal darstellen. In diese Richtung gehörend, hat man die folgende nützliche Eigenschaft.

LEMMA 1.1 (Jacobinski [14], Bergé [2]). *Für alle Zahlen i und j gilt*

$$\mathcal{A}(E[G_{L/K}]; i, j) = \mathcal{A}(E[G_{L/K}^{(0)}]; i, j) \otimes_{\mathcal{O}_E[G_{L/K}^{(0)}]} \mathcal{O}_E[G_{L/K}].$$

Wir können also ohne Einschränkungen voraussetzen, daß L/K reinverzweigt ist. Für jede abelsche Gruppe Γ bezeichnen wir mit $\Gamma^\dagger$ die Charaktergruppe $Hom(\Gamma, \mathbb{Q}_p^c)$. Die $\mathcal{O}_K$-Algebra $\mathcal{O}_K[C_{L/K}]$ ist vollständig zerlegbar, d.h. die Menge der Idempotente $\{e_\chi : \chi \in C_{L/K}^\dagger\}$ stellt eine $\mathcal{O}_K$-Basis dar. Daher kann jedes $\mathcal{O}_K[G_{L/K}]$-Gitter X als direkte Summe von isotypischen Faktoren $\{X_\chi := Xe_\chi : \chi \in C_{L/K}^\dagger\}$ zerlegt werden. Insbesondere gilt

$$\mathcal{A}(K[G_{L/K}^{(0)}]; i, j) = \bigoplus_{\chi \in C_{L/K}^\dagger} \mathcal{A}(K[P_{L/K}]; i, j)_\chi e_\chi,$$

wobei für jeden Charakter $\chi \in C_{L/K}^\dagger$ und jeden Unterkörper $E \subseteq K$, $\mathcal{A}(E[P_{L/K}]; i, j)_\chi$ die Menge von Element λ von $E[P_{L/K}]$ bezeichnet, die die Bedingung $\lambda(\mathfrak{p}_L^i e_\chi) \subseteq \mathfrak{p}_L^j$ erfüllen.

Der Einfachheit halber wählen wir jetzt einen absolut unverzweigten Unterkörper E von K und untersuchen das Gitter $\mathcal{A}(E[P_{L/K}]; i, j)_\chi$. Abgesehen vom Fall, daß K selbst absolut unverzweigt ist, ist eine solche Einschränkung ebenfalls durch den Versuch motiviert, Analogien zu bekannten Restultaten in der globalen, zahmen Situation zu erhalten. Hier hat es sich als notwendig herausgestellt, mit Operatoren aus dem rationalen Gruppenring zu arbeiten ([12]).

Zur Abkürzung soll im folgenden $\mathcal{O} = \mathcal{O}_E$ geschrieben werden. Da $\mathcal{O}$ absolut unverzweigt ist, wird die maximale $\mathcal{O}$-Ordnung von $E[P_{L/K}]$ als $\mathcal{O}[P_{L/K}]$-Modul von Untergruppenidempotenten erzeugt. Der Fall, daß $P_{L/K}$ zyklisch ist, ist einfacher zu behandeln, da hier die Gitter von Untergruppen eine lineare Ordnung haben. Tatsächlich kann man für ziemlich große Klassen von zyklischen Erweiterungen (falls etwa $e_K = 1$ gilt) explizite Beschreibungen der Gitter $\mathcal{A}(E[P_{L/K}]; i, j)_\chi$ finden ([1], [4]). Im allgemeinen hängt jedoch jedes dieser Gitter in einer subtilen Weise von der Arithmetik der Erweiterung L/K ab. Abgesehen von einigen Spezialfällen, die man *ad hoc* behandelt (cf. etwa [1], [4], [6], [22]), gibt es immer noch keine expliziten Resultate.

In dieser Arbeit werden wir untersuchen, inwieweit die Menge der assoziierten Ordnungen zu gebrochenen Idealen als Teilmenge aller abstrakten $\mathcal{O}$-Ordnungen in $E[P_{L/K}]$ in irgendeiner Weise ausgezeichnet ist. Das beste Resultat in dieser Richtung ist von Borevich und Vostokov. In [3] und [23], [24] wird bewiesen, daß es im Fall einer reinverzweigten abelschen p-Erweiterung ($p \geqslant 3$) genau dann gebrochene $\mathcal{O}_L$-Ideale gibt, die zerlegbare $\mathcal{O}_K[G_{L/K}]$-Moduln sind, wenn der Verzweigungsindex von L/K ein Teiler der Differente $\mathcal{D}_{L/K}$ von L/K ist. Falls also L/K eine abelsche, nicht-zyklische Erweiterung und ε das Trivialelement von $C^\dagger_{L/K}$ ist, so kann die Ordnung $\mathcal{A}(K[P_{L/K}]; k)_\varepsilon$ keine nicht-trivialen Idempotente enthalten. Später hat Fröhlich unter Verwendung der kanonischen Faktoräquivalenz zwischen $\mathcal{O}_L$ und $\mathcal{O}_K[G_{L/K}]$ beobachtet, daß für jeden Charakter $\chi \in C^\dagger_{L/K}$ die Ordnung $\mathcal{A}(E[P_{L/K}]; 0)_\chi$ nicht maximal ist (siehe etwa [13], (2.4)). Während der Beweis von Borevich und Vostokov sehr technisch und speziell auf p-Gruppen zugeschnitten ist, ist Fröhlichs Resultat von indextheoretischer Natur und führt nicht zu einer tieferen Analyse der assoziierten Ordnungen.

In diesem Artikel benutzen wir nur einfache Verzweigungstheorie um zu zeigen, daß im Fall $p \geqslant 3$ für jede Zahl k und jeden Charakter $\chi \in C^\dagger_{L/K}$ die Ordnung $\mathcal{A}(E[P_{L/K}]; k)_\chi$ keine nicht-trivialen Idempotente enthalten kann. Für jede Primzahl $p \geqslant 3$ ist dieses Resultat offensichtlich viel stärker und allgemeiner als Fröhlichs Bemerkung. Für $e_K > 1$ ist es jedoch *a priori* schwächer als eine Aussage über die Unzerlegbarkeit. Das Resultat gilt nicht im Fall $p = 2$.

Aus unseren Betrachtungen zu den Idempotenten in § 3 wird ersichtlich, daß eine explizite Beschreibung assoziierter Ordnungen selbst im einfachsten nicht-zyklischen Fall sehr schwer ist. Daher stellen wir in Abschnitt 4 ein Verfahren zur expliziten Berechnung von assoziierten Ordnungen vor. Dieses Verfahren wurde unter Verwendung des Programmsystems KANT ([19]) auf einem Rechner implementiert. Als konkrete Anwendung unseres Algorithmus berechnen wir alle auftretenden assoziierten Ordnungen in einer gewissen voll wildverzweigten Galoiserweiterung vom Grad 9.

Insbesondere erhalten wir ein Gegenbeispiel zu einer Vermutung des zweitgenannten Autors in [4], § 4.3 (siehe auch [5]).

Die Idee zu dieser Arbeit entstand während eines gemeinsamen Forschungsaufenthalts im Februar 1994 am Fields Institut in Waterloo, Kanada. Die Autoren möchten sich an dieser Stelle sehr herzlich bei den Mitarbeitern des Fields Instituts für ihre Gastfreundschaft bedanken.

2. Einige Vorbemerkungen

Wir setzen ab jetzt voraus, daß L/K fest gewählt ist. Zur Abkürzung soll $G^{(i)} = G^{(i)}_{L/K}$, $G_{i(i)} = G_{L/K,\,(i)}$, und $C = C_{L/K}$ geschrieben werden. Ferner setzen wir auch $P = G^{(1)}$ und $r = \# C$.

Da $\mathcal{O}/\mathbb{Z}_p$ unverzweigt ist, werden die primitiven Komponenten der Wedderburnzerlegung der E-Algebra $E[P]$ durch die Klasseneinteilung von $P^\dagger$ parametrisiert. Dabei gehören zwei Charaktere derselben Klasse an, wenn sie dieselbe zyklische Untergruppe von $P^\dagger$ erzeugen. Da sämtliche Charaktere einer Klasse D denselben Kern haben, setzen wir $Q_D = \ker \chi$ für einen beliebigen Charakter $\chi \in D$. Im Fall $Q_D \neq P$ sei Q'_D die eindeutig bestimmte Untergruppe von P mit $Q_D < Q'_D \leqslant P$ und $\#(Q'_D/Q_D) = p$. Die primitiven Idempotente von $E[P]$ sind nun durch das zur trivialen Klasse gehörende Idempotent e_P, sowie durch die Idempotente $e_D := e_{Q_D} - e_{Q'_D}$ für jede nicht-triviale Klasse D, gegeben. Für alle Klassen D wählen wir ein Element $g_D \in P \backslash Q_D$, das die Bedingung

$$P = Q_D \langle g_D \rangle$$

erfüllt und setzen $f_D = g_D - 1$. Sei $\mathcal{M}(\mathcal{O}, P)$ die maximale $\mathcal{O}$-Ordnung in $E[P]$. Die folgende Tatsache ist wohlbekannt (und einfach zu beweisen).

Lemma 2.1. *Für jede Klasse D hat die Ordnung $\mathcal{M}(\mathcal{O}, P)\, e_D$ als $\mathcal{O}$-Basis die Menge*

$$\{ f_D^i e_D : 0 \leqslant i \leqslant \# D - 1 \}.$$

Wegen

$$\mathcal{A}(E[P]; k)_\chi \subseteq \mathcal{M}(\mathcal{O}, P) = \bigoplus_D \mathcal{M}(\mathcal{O}, P)\, e_D$$

und Lemma 2.1 gilt unser Hauptinteresse zunächst den Untergruppenidempotenten und den Elementen von $\mathcal{O}[P]$ mit Augmentation Null. Dazu müssen wir etwas genauer auf die Charaktergruppe $C^\dagger$ eingehen. Sei Π ein

uniformisierender Parameter für L. Die Abbildung $g \mapsto \Pi^g/\Pi$ (wobei $g \in G$) induziert einen von der Wahl von Π unabhängigen Isomorphismus θ_0 zwischen C und einer Untergruppe der Einheitswurzeln des Restklassenkörpers von K. Sei θ das eindeutig bestimmte Element von $C^\dagger$, das den Isomorphismus θ_0 liefert. Also wird $C^\dagger$ von θ erzeugt und man kann jedem Charakter $\chi \in C^\dagger$ durch die Bedingung

$$\chi = \theta^{-u_\chi}$$

eindeutig eine Zahl

$$u_\chi \in \{1, 2, ..., r\}$$

zuordnen. Sei v_L die normierte Bewertung von L. Für jeden Charakter $\chi \in C^\dagger$ und jede Teilmenge $X \subseteq L$, die der Bedingung $e_\chi(X) \neq 0$ genügt, definieren wir

$$m_{L,\chi}(X) := \text{Minimum}\{v_L(e_\chi x) : x \in X\}.$$

LEMMA 2.2. (i) *Ist χ ein Element von $C^\dagger$, so gilt für jedes von Null verschiedene Element x der Menge $e_\chi(L)$*

$$v_L(x) \equiv -u_\chi \text{ modulo } (r).$$

Insbesondere gilt für jedes $k \in \mathbb{Z}$

$$m_{L,\chi}(\mathfrak{p}_L^k) = k + \delta_{L,\chi}(k),$$

wobei $\delta_{L,\chi}(k)$ durch $0 \leqslant \delta_{L,\chi}(k) \leqslant r-1$ und $k + \delta_{L,\chi}(k) \equiv -u_\chi$ modulo (r) eindeutig festgelegt ist.

(ii) *Ist H eine Untergruppe von G und $F = L^H$, so gilt*

$$v_F(Tr_H(I)) = \left[\frac{1}{\#H} \left(v_L(I) + \sum_{i \geqslant 0} (\#(G_{(i)} \cap H) - 1) \right) \right]$$

und

$$v_F(I^H) = \left[\frac{v_L(I)}{\#H} \right].$$

(iii) *Im Fall $g \in G_{(i)} \backslash G_{(i+1)}$ und $m_{L,\chi}(\mathfrak{p}_L^k) = d$ gilt*

$$m_{L,\chi}((g-1)\,\mathfrak{p}_L^k) = \begin{cases} d + r + i, & \text{falls } p \mid d, \\ d + i, & \text{falls } p \nmid d. \end{cases}$$

(iv) *Für $\#G = p$ ist die Sprungnummer von $\{G_{L/K}^{(i)}\}_{i \geqslant 0}$ durch $e_K p/(p-1)$ beschränkt.*

Beweis. Aus der Definition von θ folgt, daß für jedes von Null verschiedene Element $x \in L$ die Ungleichung $v_L(e_\chi x) \geqslant v_L(x)$ gilt, mit Gleichheit genau dann, wenn $\chi = \theta^{v_L(x)}$. Hieraus leitet sich die Aussage (i) ab. Die Punkte (ii) und (iii) sind wohlbekannt und (iv) ist das Resultat von etwa ([20], IV, § 2, Exercise 3). ▮

3. Zu den Idempotenten

In diesem Abschnitt beweisen wir

Satz 3.1. *Sei $k \in \mathbb{Z}$, $p \geqslant 3$ eine Primzahl und P eine abelsche, nicht-zyklische p-Gruppe. Dann enthält die Ordnung $\mathscr{A}(E[P]; k)_\chi$ keine nicht-trivialen Idempotente.*

Wie das folgende Beispiel zeigt, ist dieses Resultat im Fall $p = 2$ falsch.

Beispiel 3.2. *Sei $L/\mathbb{Q}$ eine absolut-abelsche Erweiterung, die ein gebrochenes $\mathcal{O}_L$-Ideal A_L mit $A_L^2 = \mathscr{D}_{L/\mathbb{Q}}^{-1}$ hat. Selbst im Fall, daß die Verzweigungsgruppe I an der Stelle $p = 2$ nicht-zyklisch ist, läßt dieses Ideal A_L die maximale $\mathbb{Z}$-Ordnung von $\mathbb{Q}[I]$ als Operatorenring zu* (*siehe etwa* ([9], *Appendix A*)).

Wir führen den Beweis von Satz 3.1 auf den einfachsten Fall zurück

Lemma 3.3. *Sei p eine Primzahl* (*ohne Einschränkung*). *Ist P abelsch und nicht-zyklisch und $\mathscr{A}(E[P]; k)_\chi$ eine Ordnung, die ein nicht-triviales Idempotent enthält, dann gibt es einen nicht-zyklischen Subquotienten $\bar{P}$ der Ordnung p^2 von P und eine Ordnung $\mathscr{A}(E[\bar{P}]; l)_\chi$, die ebenfalls ein nicht-triviales Idempotent enthält.*

Beweis. Wir beweisen Lemma 3.3 durch Induktion nach $\#P$. Ist I ein gebrochenes $\mathcal{O}_L$-Ideal, das eine Wirkung von einem Idempotenten $e \in E[P]$ zuläßt, dann ist für jede Untergruppe $R \leqslant P$ das gebrochene $\mathcal{O}_{L^R}$-Ideal $e_R I$ stabil unter der Wirkung des Idempotenten $ee_R \in E[P]\, e_R = E[P/R]$. Es genügt also im Fall $\#P \geqslant p^3$ zu beweisen, daß es für jedes nicht-triviale Idempotent $e \in E[P]$ entweder eine Untergruppe $R < P$ gibt, für die die Faktorgruppe P/R nicht-zyklisch ist und für die $ee_R \neq 0$ und $ee_R \neq e_R$ gilt, oder aber daß e bereits in $E[P']$ für eine echte, nicht-zyklische Untergruppe P' von P enthalten ist.

Zuerst nehmen wir an, daß für jede Untergruppe Q der Ordnung p die Faktorgruppe P/Q nicht-zyklisch ist. Nun gibt es wegen $e \neq 0$ eine Untergruppe R_0 der Ordnung p, die die Bedingung $ee_{R_0} \neq 0$ erfüllt. Im Fall

$ee_{R_0} \neq e_{R_0}$ sind wir fertig. Im Fall $ee_{R_0} = e_{R_0}$ folgt, daß das primitive Idempotent e_P in e enthalten ist. Dann gilt aber $ee_R \neq 0$ für alle Untergruppen R der Ordnung p. Wir führen nun den Beweis indirekt. Angenommen es gilt $ee_R = e_R$ für alle Untergruppen der Ordnung p. Dann sind aber alle primitiven Idempotente in e enthalten und deshalb gilt $e = 1$-Widerspruch.

Wir betrachten nun den Fall, daß es eine Untergruppe R der Ordnung p gibt, für die die Faktorgruppe P/R zyklisch ist. In diesem Fall gilt $P = \langle a \rangle \times \langle b \rangle$, wobei a (bzw. b) ein Element der Ordnung $p^m (m > 1)$ (bzw. p) bezeichnet. Nun setzen wir $R_0 = P^{p^{m-1}} = \langle a^{p^{m-1}} \rangle$. Da P/R_0 nicht-zyklisch ist, nehmen wir an, daß entweder $ee_{R_0} = 0$ oder $ee_{R_0} = e_{R_0}$ ist. Andererseits kann man zeigen, daß $1 - e_{R_0}$ eine Summe von primitiven Idempotenten von $E[P]$ ist, die in $E[\langle a^{p^{m-1}}, b \rangle]$ enthalten sind. Also läßt in diesem Fall das Ideal I eine Wirkung des Idempotents $e = ee_{R_0} + e(1 - e_{R_0}) \in E[\langle a^{p^{m-1}}, b \rangle]$ zu. Die Gruppe $\langle a^{p^{m-1}}, b \rangle$ ist aber nicht-zyklisch der Ordnung p^2. ∎

Es genügt also, Satz 3.1 im Spezialfall P nicht-zyklisch der Ordnung p^2 zu beweisen. Für solche Erweiterungen werden die $p+1$ Untergruppen von P der Ordnung p mit $P_1, P_2, ..., P_{p+1}$ bezeichnet. Für die zugehörigen Untergruppenidempotente e_{P_i} schreiben wir kurz e_i. Für jede Zahl $i \in \{1, 2, ..., p+1\}$ wählt man ein Element $g_i' \in P_i \backslash \{1\}$ (bzw. $g_i \in P \backslash P_i$) und setzt $f_i' = g_i' - 1$ (bzw. $f_i = g_i - 1$). Seien u_1, u_2 die (möglicherweise gleichen) Sprungnummern der Verzweigungsgruppenreihe $\{G^{(i)}\}_{i \geq 1}$. Lemma 2.2(iv) liefert nun $u_i = (e_K p - \delta_i)/(p-1)$ für eine nicht negative ganze Zahl δ_i, $i = 1, 2$.

LEMMA 3.4. *Sei $p \geq 3$ eine Primzahl, P eine nicht-zyklische Gruppe der Ordnung p^2 und $\mathscr{A}$ eine Ordnung vom Typ $\mathscr{A}(E[P]; k)_\chi$.*
Sei zunächst $p \geq 5$. Dann gilt:

$$\text{(i)} \qquad f_i^{p-3} e_i \notin \mathscr{A}, \qquad \text{falls} \quad P_i \neq G^{(u_1+1)},$$

$$\text{(ii)} \qquad f_i^{p-4} e_i \notin \mathscr{A}, \qquad \text{falls} \quad P_i = G^{(u_1+1)}.$$

Sei jetzt $p = 3$ und entweder $e_K \geq 3$ oder aber $e_K = 2$ und $u_2 \neq 3$. Dann gilt:

$$\text{(iii)} \qquad f_i e_i \notin \mathscr{A}, \qquad \text{falls} \quad P_i \neq G^{(u_1+1)},$$

$$\text{(iv)} \qquad e_i \notin \mathscr{A} \quad \text{und} \quad e_i - e_P \notin \mathscr{A}, \qquad \text{falls} \quad P_i = G^{(u_1+1)}.$$

Ferner gilt für alle $p \geq 3$ stets

$$\text{(v)} \qquad e_p \notin \mathscr{A}.$$

Bevor wir dieses Lemma beweisen, zeigen wir zunächst, wie daraus zusammen mit Lemma 3.3 der Satz 3.1 im Großteil der Fälle folgt.

FOLGERUNG 3.5. *Sei $p \geqslant 3$, P eine nicht-zyklische Gruppe der Ordnung p^2 und $\mathscr{A}$ eine Ordnung vom Typ $\mathscr{A}(E[P]; k)_\chi$. Im Fall $p = 3$ gelte zusätzlich entweder $e_K \geqslant 3$ oder $e_K = 2$ und $u_2 \neq 3$. Dann enthält $\mathscr{A}$ keine nichttrivialen Idempotente.*

Beweis. Jedes Idempotent von $E[P]$ ist vom Typ

$$\alpha = \delta_{0,\alpha} e_P + \sum_{i=1}^{p+1} \delta_{i,\alpha}(e_i - e_P),$$

wobei

$$\{\delta_{i,\alpha} : 0 \leqslant i \leqslant p+1\} \subseteq \{0, 1\}.$$

Sei nun α ein fest gewähltes Idempotent. Wir nehmen an, daß $\alpha \in \mathscr{A}$ gilt, und werden zeigen, daß hieraus entweder $\alpha = 0$ oder $\alpha = 1$ folgt. Wir setzen

$$c := \#\{i : 1 \leqslant i \leqslant p+1, \delta_{i,\alpha} = 1\}.$$

Wegen

$$e_P + \sum_{i=1}^{p+1} (e_i - e_P) = 1 \in \mathscr{A},$$

kann man $c \leqslant 2^{-1}(p+1)$ annehmen. Ist $c = 0$ und $\alpha \neq 0$, so gilt $\alpha = e_P$-ein Widerspruch zu Lemma 3.4(v). Ist andererseits $c = 1$, so gilt entweder $\alpha = e_i$ oder $\alpha = e_i - e_P$ (für ein $i \in \{1, 2, ..., p+1\}$), und daher $f_i e_i = f_i \alpha \in \mathscr{A}$. Dies widerspricht aber Lemma 3.4(i), (ii), (iii) oder (iv). Also ist $c > 1$. Nun können wir sowohl $\delta_{i,\alpha} = 1$ für jedes $i \in \{1, 2, ..., c\}$ als auch $P_c \neq G^{(u_1+1)}$ annehmen. Also

$$\alpha \in \mathscr{A} \Rightarrow \left(\prod_{i=1}^{c-1} f_i'\right)\alpha = \left(\prod_{i=1}^{c-1} f_i'\right) e_c \in \mathscr{A}.$$

Andererseits gilt

$$\prod_{i=1}^{c-1} f_i' e_c \equiv u f_c^{c-1} e_c \qquad \text{modulo} \quad f_c^c e_c \mathscr{O}[P],$$

wobei $u \in \mathscr{O}^*$ eine Einheit bezeichnet. Hieraus folgt $f_c^{c-1} e_c \in \mathscr{A}$. Wegen $c \leqslant 2^{-1}(p+1)$ steht dies jedoch entweder im Widerspruch zu (i) oder (iii) aus Lemma 3.4. ∎

Beweis von Lemma 3.4. Alle diese Aussagen folgen aus einfachen Bewertungsberechnungen. Wir beweisen hier nur (i), (iii), und (iv). (Der Beweis von (ii) verläuft ähnlich wie derjenige von (i) und (v) folgt mittels einer leichten Rechnung unmittelbar aus 2.2.)

Seien die Zahl k und der Character χ fest gewählt. Zur Abkürzung sollen im folgenden $X_i = e_i(\mathfrak{p}_L^k)$, $L_i = L^{P_i}$, $\mathfrak{p}_i = \mathfrak{p}_{L_i}$, $\Gamma_i = G/P_i$, $Q_i = P/P_i$, $v_i(-) = v_{L_i}(-)$, und $m_{i,\chi}(-) = m_{L_i,\chi}(-)$ geschrieben werden. Außerdem setzen wir $L_0 = L^P$. Die einzige Sprungnummer von $\{\Gamma_i^{(j)}\}_{j \geqslant 1}$ ist u_1, falls $P_i = G^{(u_1+1)}$, bzw. u_2, falls $P_i \neq G^{(u_1+1)}$. Deshalb ist die Verzweigungsgruppenreihe in unterer Numerierung von Γ_i durch

$$\Gamma_i = \Gamma_{i(0)} \geqslant \Gamma_{i(1)} = \cdots = \Gamma_{i(ru_1)} = Q_i > \Gamma_{i(ru_1+1)} = 1,$$

bzw.

$$\Gamma_i = \Gamma_{i(0)} \geqslant \Gamma_{i(1)} = \cdots = \Gamma_{i(ru_2)} = Q_i > \Gamma_{i(ru_2+1)} = 1$$

gegeben. Insbesondere erfüllt jedes nicht-triviale Element q aus Q_i die Bedingung

$$q \in \begin{cases} \Gamma_{i(ru_1)} \backslash \Gamma_{i(ru_1+1)}, & \text{falls} \quad P_i = G^{(u_1+1)}, \\ \Gamma_{i(ru_2)} \backslash \Gamma_{i(ru_2+1)}, & \text{falls} \quad P_i \neq G^{(u_1+1)}. \end{cases} \tag{1}$$

Aus Lemma 2.2(i) und (ii) folgert man im Fall $P_i \neq G^{(u_1+1)}$ die Ungleichungen

$$\begin{aligned} m_{i,\chi}(X_i) &= \left\lceil \frac{k + (1+u_1 r)(p-1)}{p} \right\rceil - e_K p r + \delta_{L_i,\chi}(v_i(X_i)) \\ &\leqslant \left\lceil \frac{k + p - 1 - u_1 r}{p} \right\rceil + u_1 r - e_K p r + r - 1 \\ &\leqslant \left\lceil \frac{k}{p} \right\rceil + u_1 r - e_K p r + r - 1. \end{aligned} \tag{2}$$

Zur Aussage (i): Da die L_i-Bewertung von $(\mathfrak{p}_L^k)^{P_i}$ durch $\lceil p^{-1}k \rceil$ gegeben ist (Lemma 2.2(ii)), genügt es zu zeigen, daß $m_{i,\chi}(f_i^{p-3} X_i) < \lceil p^{-1}k \rceil$ ist. Nun sind drei Fälle zu unterscheiden:

(α) Fall: $p \nmid m_{i,\chi}(X_i)$;

(β) Fall: $p \mid m_{i,\chi}(X_i)$ und $p \nmid u_2$;

(γ) Fall: $p \mid m_{i,\chi}(X_i)$ und $p \mid u_2$.

Fall (α): In diesem Fall benutzen wir die Kongruenz

$$f_i^p \equiv -p f_i \text{ modulo } (p f_i^2 \mathcal{O}[P]).$$

Aus dieser Kongruenz folgt zusammen mit Lemma 2.2 (iii)

$$m_{i,\chi}(f_i^p X_i) = m_{i,\chi}(f_i X_i) + v_i(p) = m_{i,\chi}(X_i) + u_2 r + e_K p r,$$

und daher

$$m_{i,\chi}(f_i^{p-3}X_i) \leqslant m_{i,\chi}(f_i^p X_i) - 3u_2 r = (m_{i,\chi}(X_i) + u_2 r + e_K pr) - 3u_2 r.$$

Aber nach (2) ist diese Zahl kleiner oder gleich

$$\left\lceil \frac{k}{p} \right\rceil + r - 1 + (u_1 - u_2)\, r - u_2 r < \left\lceil \frac{k}{p} \right\rceil.$$

Fall (β): Nun ist $\delta_2 > 0$. In diesem Fall betrachten wir das $\mathcal{O}_{L_i}$-Ideal $X_i' = X_i \mathfrak{p}_i^{u_2 r}$. Da $m_{i,\chi}(X_i') = m_{i,\chi}(X_i) + u_2 r \equiv u_2 r$ modulo (p) ist, folgt aus Lemma 2.2 (iii) zusammen mit (1)

$$m_{i,\chi}(f_i^{p-3}X_i') = m_{i,\chi}(X_i') + (p-3)\, u_2 r.$$

Also gilt

$$\begin{aligned}
m_{i,\chi}(f_i^{p-3}X_i) &\leqslant m_{i,\chi}(f_i^{p-3}X_i') \\
&= m_{i,\chi}(X_i) + u_2 r + (p-3)\, u_2 r \\
&\leqslant \left\lceil \frac{k}{p} \right\rceil + u_1 r - e_K pr + r - 1 + u_2 r + (p-3)\, u_2 r \text{ (wegen (2))} \\
&\leqslant \left\lceil \frac{k}{p} \right\rceil - e_K pr + r - 1 + (p-1)\, u_2 r \\
&= \left\lceil \frac{k}{p} \right\rceil - e_K pr + r - 1 + e_K pr - \delta_2 r \\
&= \left\lceil \frac{k}{p} \right\rceil + r(1 - \delta_2) - 1.
\end{aligned}$$

Wegen $\delta_2 > 0$ ist diese Zahl kleiner als $\lceil p^{-1}k \rceil$.

Fall (γ): In diesem Fall betrachten wir das $\mathcal{O}_{L_i}$-Ideal $X_i'' = X_i \mathfrak{p}_i^r$. Da $u_2 \equiv 0$ modulo p ist, folgt aus Lemma 2.2 (iii) zusammen mit (1), daß $m_{i,\chi}(f_i^s X_i'') \equiv r$ modulo p für jede Zahl $s \geqslant 0$ gilt. Also ergibt sich

$$\begin{aligned}
m_{i,\chi}(f_i^{p-3}X_i) &\leqslant m_{i,\chi}(f_i^{p-3}X_i'') \\
&= m_{i,\chi}(X_i'') + (p-3)\, u_2 r \\
&= m_{i,\chi}(X_i) + r + (p-3)\, u_2 r,
\end{aligned}$$

und aus (2) folgt, daß diese Zahl kleiner oder gleich

$$\left\lceil \frac{k}{p} \right\rceil + u_1 r - e_K pr + r - 1 + r + (p-3)\, u_2 r \tag{3}$$

ist. Nun ist

$$\begin{aligned} u_1 r - e_K pr + r - 1 + r + (p-3)\, u_2 r &\leqslant -e_K pr + 2r - 1 + (p-2)\, u_2 r \\ &\leqslant -e_K pr + 2r - 1 + (pe_K - \delta_2)\, r - u_2 r \\ &= (2 - \delta_2 - u_2)\, r - 1, \end{aligned}$$

und diese Zahl ist wegen $p \mid u_2$ negativ. Also ist die Zahl in (3) kleiner als $\lceil p^{-1}k \rceil$.

Zu den Aussagen (iii) *und* (iv). Aus Lemma 2.2 (iii) und (1) folgert man $m_{i,\chi}(f_i X_i) \leqslant m_{i,\chi}(X_i) + r + u_2 r$, und daher liefert die Ungleichung (2) im Fall $P_i \neq G^{(u_1+1)}$

$$\begin{aligned} m_{i,\chi}(f_i X_i) &\leqslant \left\lceil \frac{k + (1 + u_1 r)(p-1)}{p} \right\rceil - pe_K r + r - 1 + r + u_2 r \\ &< \left\lceil \frac{k + 2 + (3e_K - \delta_2)\, r}{3} \right\rceil - 3e_K r + 2r + \left(\frac{3e_K - \delta_2}{2} r \right) \\ &= \left\lceil \frac{k + 2 - \delta_2 r}{3} \right\rceil - \left(2e_K - 2 - \frac{3e_K - \delta_2}{2} \right) r. \end{aligned}$$

Hierans folgt nun $m_{i,\chi}(f_i X_i) < \lceil k/3 \rceil$, falls $2e_K - 2 - (3e_K - \delta_2)/2 \geqslant 0$ gilt. Diese letztere Bedingung ist für $e_K \geqslant 4$ offensichtlich erfüllt, aber auch für $e_K = 3$, da dann δ_2 ungerade ist. Im Fall $e_K = 2$ gilt $\delta_2 \in \{0, 2, 4\}$ und die geforderte Ungleichung wird außer für $\delta_2 = 0$ (was $u_2 = 3$ bedeutet) erfüllt. Damit ist (iii) gezeigt.

Zur Behandlung des Falls $P_i = G^{(u_1+1)}$ notieren wir folgendes

LEMMA 3.6. *Sei* $p = 3$ *und* $P_i = G^{(u_1+1)}$. *Dann gilt*:

$$e_i \notin \mathscr{A} \qquad \text{und} \qquad e_i - e_P \notin \mathscr{A}.$$

Beweis. Aus Lemma 2.2(i) and (ii) folgt die Ungleichung

$$\begin{aligned} m_{i,\chi}(X_i) &\leqslant \left\lceil \frac{k + (1 + u_1 r + p(u_2 - u_1)\, r)(p-1)}{p} \right\rceil - pe_K r + r - 1 \\ &= \left\lceil \frac{k + 2 - u_1 r}{3} \right\rceil + u_1 r + 2(u_2 - u_1)\, r - 3e_K r + r - 1. \end{aligned}$$

Dies impliziert $m_{i,\chi}(X_i) < \lceil k/3 \rceil$, falls $u_1 r + 2(u_2 - u_1) r - 3e_K r + r \leqslant 0$ gilt. Diese letztere Ungleichung ist wiederum eine einfache Konsequenz aus $1 \leqslant u_1$, $u_2 \leqslant 3e_K/2$. Damit gilt also $e_i \notin \mathscr{A}$.

Es ist nun noch $e_i - e_P \notin \mathscr{A}$ zu zeigen. Wir nehmen $e_i - e_P \in \mathscr{A}$ an und führen den Beweis indirekt. Es folgt nun wegen $e_i \notin \mathscr{A}$ und $e_P \notin \mathscr{A}$ die Gleicheit $m_{i,\chi}(X_i) = pm_{0,\chi}(e_{Q_i} X_i)$. Aber L_i/L_0 hat die Sprungnummer $u_1 r$, woraus man

$$\begin{aligned} v_0(e_{Q_i} \mathfrak{p}_i^{m_{i,\chi}(X_i)+r}) &= \left\lceil \frac{m_{i,\chi}(X_i) + r + (1 + u_1 r)(p-1)}{p} \right\rceil - e_K r \\ &= m_{0,\chi}(e_{Q_i} X_i) + \left\lceil \frac{r + 2 + (3e_K - \delta_1) r}{3} \right\rceil - e_K r \\ &= m_{0,\chi}(e_{Qi} X_i) + \left\lceil \frac{r + 2 - \delta_1 r}{3} \right\rceil \end{aligned}$$

ableitet.

Wegen $u_1 < u_2$ gilt $\delta_1 \geqslant 2$ und daher $v_0(e_{Q_i} \mathfrak{p}_i^{m_{i,\chi}(X_i)+r}) \leqslant m_{0,\chi}(e_{Q_i} X_i)$. Folglich gibt es ein Element $x \in \mathfrak{p}_i^{m_{i,\chi}(X_i)+r}$ mit der Eigenschaft $v_i(e_\chi e_{Q_i} x) \leqslant pm_{0,\chi}(e_{Q_i} X_i) = m_{i,\chi}(X_i)$. Wählt man nun $y \in \mathfrak{p}_L^k$ mit $e_i y = x$, so erhält man $v_i((e_i - e_P)\, e_\chi y) = v_i(-e_{Q_i} e_\chi x) < \lceil k/3 \rceil$. Also gilt $e_i - e_P \notin \mathscr{A}$. ∎

Damit ist auch der Beweis von (iv) erbracht. ∎

Um den Beweis von Satz 3.1 zu vervollständigen, genügt es zu zeigen, daß in den von Folgerung 3.5 noch nicht erfaßten Fällen kein Element der Form e_i, $e_i - e_P$ oder $e_i + e_j - e_P$ für $i, j \in \{1, 2, 3, 4\}$, $i \neq j$, in der assoziierten Ordnung $\mathscr{A}(E[P]; k)_\chi$ enthalten sein kann.

LEMMA 3.7. *Sei* $p = 3$, $e_K = 1$ *und* P *nicht-zyklisch von der Ordnung* 9. *Dann enthält* $\mathscr{A}(E[P]; k)_\chi$ *kein Element der Form* e_i, $e_i - e_P$ *oder* $e_i + e_j - e_P$ *für* $i, j \in \{1, 2, 3, 4\}$, $i \neq j$.

Beweis. Zur Abkürzung schreiben wir wieder $\mathscr{A} = \mathscr{A}(E[P]; k)_\chi$. Wegen $e_K = 1$ hat man $u_1 = u_2 = 1$ (siehe Lemma 2.2 (iv)) und daher ist $c := m_{i,\chi}(X_i)$ unabhängig von der Wahl von $i \in \{1, 2, 3, 4\}$. Eine einfache Rechnung unter Verwendung von Lemma 2.2 (i), (ii) zeigt

$$c < \left\lceil \frac{k}{p} \right\rceil - r, \tag{4}$$

insbesondere gilt also $e_i \notin \mathscr{A}$.

Nehmen wir nun an, daß $e_i - e_P$ oder $e_i + e_j - e_P$, $i \neq j$, in $\mathscr{A}$ enthalten ist. Dann gilt auch $f_j' e_i \in \mathscr{A}$ und (4) zusammen mit Lemma 2.2 (iii) impliziert $c \equiv 0$ modulo p. Für jede ganze Zahl $\varepsilon \geqslant 0$ gilt nun

$$v_0(e_{Q_i} \mathfrak{p}_i^{c+\varepsilon r}) = \left[\frac{c + \varepsilon r + (1+r)(p-1)}{p} \right] - r$$

$$= \frac{c}{p} + \left[\frac{(\varepsilon - 1) r + p - 1}{p} \right],$$

und mittels Lemma 2.2(i) folgt hieraus

$$m_{0,\chi}(e_{Q_i} \mathfrak{p}_i^{c+\varepsilon r}) = \begin{cases} cp^{-1}, & \text{falls} \quad \varepsilon = 0, 1, \\ \geqslant cp^{-1} + r, & \text{falls} \quad \varepsilon > 1. \end{cases} \tag{5}$$

Insbesondere ergibt sich für ein $x \in L_i$ mit der Eigenschaft $v_i(x) = c + r$ unmittelbar $v_i(e_{Q_i} e_\chi x) = c$. Für ein $y \in \mathfrak{p}_L^k$ mit $v_i(e_i y) = c + r$ gilt dann

$$v_i((e_i - e_P)\, e_\chi y) = v_i(e_i e_\chi y - e_P e_\chi y) = c,$$

und daher $e_i - e_P \notin \mathscr{A}$. Außerdem kann das Gitter $(e_i - e_P)\, e_\chi \mathfrak{p}_L^k \subset L_i$ kein Element vom v_i-Wert $c + r$ enthalten. Wegen $c \equiv 0$ modulo p kann man nämlich jedes $\beta \in e_i e_\chi \mathfrak{p}_L^k$ in der Form $\beta = \beta_0 + \beta_1$ schreiben, wobei $\beta_0 \in L_0$ und $v_i(\beta_1) = c + \varepsilon r$ mit einer ganz rationalen Zahl $\varepsilon \geqslant 1$ ist. Ferner gilt aber $(e_i - e_P)\, \beta = (1 - e_{Q_i})\, \beta_1$ und aus (5) folgert man leicht, daß kein solches Element den v_i-Wert $c + r$ haben kann. Sei nun $x \in \mathfrak{p}_L^k$ und es gelte $v_i(e_j e_\chi x) = c + r$. Dann folgt

$$v_L((e_j + e_i - e_P)\, e_\chi x) = v_L(e_j e_\chi x + (e_i - e_P)\, e_\chi x)$$

$$\leqslant v_L(e_j e_\chi x) = p(c + r) < p \left\lceil \frac{k}{p} \right\rceil.$$

Also gilt $e_i + e_j - e_P \notin \mathscr{A}$ für alle $i, j \in \{1, 2, 3, 4\}$. ∎

LEMMA 3.8. *Sei* $p = 3$, $e_K = 2$, $u_2 = 3$ *und* P *nicht-zyklisch von der Ordnung* 9. *Dann enthält* $\mathscr{A}(E[P]; k)_\chi$ *kein Element der Form* e_i, $e_i - e_P$ *oder* $e_i + e_j - e_P$ *für* $i, j \in \{1, 2, 3, 4\}$, $i \neq j$.

Beweis. Sei wieder $\mathscr{A} = \mathscr{A}(E[P]; k)_\chi$ und sei c der gemeinsame Wert von $m_{i,\chi}(X_i)$ für ein $P_i \neq G^{(u_1+1)}$. Aus Lemma 2.2 folgt

$$c \leqslant \left\lceil \frac{k+(1+u_1 r)(p-1)}{p} \right\rceil - pe_K r + r - 1$$

$$< \left\lceil \frac{k+2(1+3r)}{3} \right\rceil - 6r + r$$

$$= \left\lceil \frac{k}{3} \right\rceil - 3r. \tag{6}$$

Damit erhält man für $P_i \neq G^{(u_1+1)}$ das Resultat $e_i \notin \mathscr{A}$. Nehmen wir nun an, daß ein Element $e_i - e_P$ oder $e_i + e_j - e_P$ mit $i \neq j$ in $\mathscr{A}$ enthalten ist. Dann ist auch $f'_j e_i \in \mathscr{A}$ und zusammen mit (6) und Lemma 2.2(iii) liefert dies $c \equiv 0$ modulo 3. Nun hat aber L_i/L_0 wegen $P_i \neq G^{(u_1+1)}$ die Sprungnummer $3r$ und damit läßt sich zeigen, daß $m_{i,\chi}(e_{Q_i} \mathfrak{p}_i^l) \geqslant l$ für alle $l \in \mathbb{Z}$ gilt. Als einfache Konsequenz hieraus erhält man $m_{i,\chi}((e_i - e_P)\, \mathfrak{p}_L^k) = c + r$ und damit $e_i - e_P \notin \mathscr{A}$. Es gelte nun zusätzlich $P_j \neq G^{(u_1+1)}$, $i \neq j$. Für $x \in \mathfrak{p}_L^k$ mit $v_j(e_j e_\chi x) = c$ folgt jetzt

$$v_L((e_j + e_i - e_P)\, e_\chi x) = v_L(e_j e_\chi x) = 3c < k$$

und daher $e_j + e_i - e_P \notin \mathscr{A}$.

Letzlich bleibt nur noch der Fall $P_{i_0} = G^{(u_1+1)}$ zu betrachten. Wegen Lemma 3.6 genügt es $e_{i_0} + e_i - e_P \notin \mathscr{A}$ für alle $i \in \{1, 2, 3, 4\} \setminus \{i_0\}$ zu zeigen. In diesem Fall findet man durch eine einfache Rechnung $m_{i_0,\chi}(X_{i_0}) > c + r = m_{i,\chi}((e_i - e_P)\, \mathfrak{p}_L^k)$, und hieraus folgert man

$$m_{L,\chi}((e_{i_0} + e_i - e_P)\, \mathfrak{p}_L^k) = p(c+r) < k. \quad \blacksquare$$

4. Ein Algorithmus

In Anbetracht der vielen technischen Schwierigkeiten im Beweis von Satz 3.1 scheint die Berechnung von assoziierten Ordnungen im allgemeinen ein fast hoffnungsloses Problem darzustellen. Daher ist es sehr nützlich einen effektiven Algorithmus zur Hand zu haben, um an konkreten Beispielen mögliche Hypothesen zu testen. Ein solches Verfahren zur numerischen Berechnung assoziierter Ordnungen wollen wir in diesem Abschnitt vorstellen.

Sei R im folgenden stets ein Hauptidealring. Wir bezeichnen mit M den Quotientenkörper von R. Sei weiter N eine endliche, galoissche Erweiterung von M vom Grade n mit Galoisgruppe $G = G_{N/M}$.

Sei nun $X \subseteq N$ ein volles $R[G]$-Gitter auf N. Die assoziierte Ordnung $\mathcal{A}(X)$ von X wird in der üblichen Weise definiert:

$$\mathcal{A}(X) = \{\lambda \in M[G] \mid \lambda(X) \subseteq X\}.$$

Ziel dieses Abschnittes ist es nun, einen Algorithmus zur expliziten Berechnung der Ordnung $\mathcal{A}(X)$ zu entwickeln. Natürlich ist es dazu notwendig, den Modul X, sowie die vom ihm induzierte Darstellung der Gruppe G, explizit zu kennen. Daher nehmen wir für das weitere an, daß X durch eine R-Basis $\omega_1, ..., \omega_n$ gegeben ist. Die durch diese Basiswahl festgelegten Darstellungsmatrizen für $\sigma \in G$ bezeichnen wir mit $A(\sigma)$, also

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}^{\sigma} = A(\sigma) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}, \qquad A(\sigma) \in Gl_n(R).$$

Sei nun $\theta = \sum_{j=1}^{n} t_j \omega_j$, $t_j \in R$, ein Element von X, das eine Normalbasis von N/M erzeugt. Wir bezeichnen mit $\mathcal{A}_\theta$ das wie folgt definierte $R[G]$-Teilgitter von $M[G]$:

$$\mathcal{A}_\theta = \{\lambda \in M[G] \mid \lambda(\theta) \in X\}.$$

Das Verfahren zur Berechnung der assoziierten Ordnung $\mathcal{A}(X)$ beruht nun ganz wesentlich auf folgendem

LEMMA 4.1. (i) *$\mathcal{A}_\theta$ ist ein $\mathcal{A}(X)$-Linksideal im Sinne von* [8], *VI*, § 1, *Definition* 3.

(ii) *Die assoziierte Ordnung $\mathcal{A}(X)$ ist der Linksmultiplikatorenring von $\mathcal{A}_\theta$,*

$$\mathcal{A}(X) = \{\lambda \in M[G] \mid \lambda \cdot \mathcal{A}_\theta \subseteq \mathcal{A}_\theta\}.$$

Beweis. Offensichtlich ist $\mathcal{A}_\theta$ ein linksseitiger $\mathcal{A}(X)$-Modul. Sei $d = [X : R[G]\,\theta]_R \in R$. Dann gilt $d\mathcal{A}_\theta \subseteq \mathcal{A}(X)$. Damit ist (i) gezeigt. Der Punkt (ii) folgt sofort aus $\mathcal{A}_\theta \theta = X$ und unserer Voraussetzung, daß θ eine Normalbasis von N/M erzeugt. Daher gilt nämlich für $\lambda \in M[G]$:

$$\lambda(X) \subseteq X \Leftrightarrow \lambda(\mathcal{A}_\theta \theta) \subseteq \mathcal{A}_\theta \theta \Leftrightarrow \lambda \mathcal{A}_\theta \subseteq \mathcal{A}_\theta.$$

(Siehe auch [11], Chapitre I, 2.) ∎

Im ersten Schritt des Algorithmus berechnen wir $\mathscr{A}_\theta$. Dazu bestimmen wir Elemente $\lambda_i \in M[G]$, die der Eigenschaft

$$\lambda_i(\theta) = \omega_i, \qquad i = 1, ..., n,$$

genügen. Da θ eine Normalbasis von N/M erzeugt, sind diese Gleichungen eindeutig lösbar und es gilt offensichtlich

$$\mathscr{A}_\theta = \langle \lambda_1, ..., \lambda_n \rangle_R.$$

Setzt man $\lambda_i = \sum_{\sigma \in G} x_\sigma \sigma$ an, so ist zur expliziten Berechnung von λ_i nur das lineare Gleichungssystem zu lösen, das durch Koeffizientenvergleich aus

$$\lambda_i(\theta) = \sum_{k=1}^{n} \left(\sum_{\sigma \in G} \left(\sum_{j=1}^{n} t_j A(\sigma)_{jk} \right) x_\sigma \right) \omega_k = \omega_i$$

entsteht.

Zur Berechnung von $\mathscr{A}(X)$ wenden wir nun Lemma 4.1 (ii) an. Es ist also der Linksmultiplikatorenring des Gitters $\mathscr{A}_\theta$ zu berechnen.

Hierzu betrachten wir die folgende nicht-ausgeartete, symmetrische Bilinearform

$$\langle \cdot, \cdot \rangle : M[G] \times M[G] \to M,$$

die durch die Festlegung

$$\langle \sigma, \tau \rangle = \begin{cases} 1, & \text{falls } \sigma\tau = 1, \\ 0, & \text{sonst,} \end{cases} \qquad \sigma, \tau \in G,$$

definiert wird. Man verifiziert leicht $\langle \lambda_1 \lambda_2, \lambda_3 \rangle = \langle \lambda_1, \lambda_2 \lambda_3 \rangle$ für $\lambda_1, \lambda_2, \lambda_3 \in M[G]$.

Für einen $R[G]$-Modul Y in $M[G]$ bezeichnen wir den R-dualen Modul mit Y^*,

$$Y^* = \{ \lambda \in M[G] \mid \langle Y, \lambda \rangle \subseteq R \}.$$

Wir berechnen zunächst die Dualbasis zu $\lambda_1, ..., \lambda_n$, welche wir mit $\lambda_1^*, ..., \lambda_n^*$ bezeichnen. Hierzu hat man für jedes $j \in \{1, ..., n\}$ das lineare Gleichungssystem

$$\langle \lambda_i, \lambda_j^* \rangle = \delta_{ij}, \qquad i = 1, ..., n,$$

zu lösen.

Sei nun $\mathscr{A}_\theta \mathscr{A}_\theta^* = \langle \lambda_i \lambda_j^* : 1 \leqslant i, j \leqslant n \rangle_R$. Wegen $1 \in \mathscr{A}_\theta$ ist $\mathscr{A}_\theta \mathscr{A}_\theta^*$ ein volles $R[G]$-Gitter auf $M[G]$. Es gilt nun das folgende

LEMMA 4.2. $\mathscr{A}_\theta \mathscr{A}_\theta^* = \mathscr{A}(X)^*$.

Beweis. Wir zeigen zunächst die Inklusion $\mathscr{A}_\theta \mathscr{A}_\theta^* \subseteq \mathscr{A}(X)^*$. Hierfür genügt es $\lambda_i \lambda_j^* \in \mathscr{A}(X)^*$ für $1 \leqslant i, j \leqslant n$ zu beweisen. Dies ergibt sich sofort aus $\langle \mathscr{A}(X), \lambda_i \lambda_j^* \rangle = \langle \mathscr{A}(X)\, \lambda_i, \lambda_j^* \rangle$ und $\mathscr{A}(X)\, \lambda_i \subseteq \mathscr{A}_\theta$. Zum Beweis der anderen Inklusion zeigen wir $(\mathscr{A}_\theta \mathscr{A}_\theta^*)^* \subseteq \mathscr{A}(X)$. Sei dazu $\xi \in (\mathscr{A}_\theta \mathscr{A}_\theta^*)^*$, d.h.

$$\langle \lambda_i \lambda_j^*, \xi \rangle \in R \tag{7}$$

für $1 \leqslant i, j \leqslant n$. Nach Lemma 4.1 (ii) haber wir $\xi \mathscr{A}_\theta \subseteq \mathscr{A}_\theta$ zu zeigen. Hierfür genügt es wiederum $\xi \lambda_i \in \mathscr{A}_\theta$, $i = 1, ..., n$, nachzuweisen. Da $\lambda_1, ..., \lambda_n$ eine Basis von $M[G]$ über M ist, gibt es eine Darstellung

$$\xi \lambda_i = \sum_{j=1}^{n} x_j \lambda_j \qquad \text{mit} \quad x_j \in M.$$

Es ist zu zeigen, daß $x_j \in R$ für $j = 1, ..., n$ gilt. Dies folgt aus (7) und

$$\langle \lambda_i \lambda_k^*, \xi \rangle = \langle \xi \lambda_i, \lambda_k^* \rangle = \sum_{j=1}^{n} x_j \langle \lambda_j, \lambda_k^* \rangle = x_k, \qquad k = 1, ..., n. \quad \blacksquare$$

Durch nochmaliges Dualiseren von $\mathscr{A}_\theta \mathscr{A}_\theta^*$ erhält man also die gesuchte assoziierte Ordnung $\mathscr{A}(X)$. In diesem Schritt liegt allerdings die Hauptschwierigkeit bei einer Implementierung des Algorithmus. Der Modul $\mathscr{A}_\theta \mathscr{A}_\theta^*$ ist durch die n^2 Erzeugenden $\lambda_i \lambda_j^*$, $1 \leqslant i, j \leqslant n$, gegeben und vor der Berechnung des dualen Moduls ist zunächst eine R-Basis von $\mathscr{A}_\theta \mathscr{A}_\theta^*$ zu finden. Sei dazu

$$\lambda_i \lambda_j^* = \sum_{\sigma \in G} c_{ij,\sigma} \sigma \qquad \text{mit} \quad c_{ij,\sigma} \in R, \quad 1 \leqslant i, j \leqslant n.$$

Die Matrix $C = (c_{ij,\sigma})_{1 \leqslant i, j \leqslant n,\, \sigma \in G} \in R^{n^2 \times n}$ kann nun auf Hermitesche Normalform gebracht werden, d.h. es gibt eine Matrix $U \in Gl_{n^2}(R)$, so daß $H(C) = UC$ obere Dreiecksgestalt hat. Wir bezeichnen die Elemente von G mit $\sigma_1, ..., \sigma_n$. Offensichlich ist dann durch

$$H(C) \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

eine Basis $v_1, ..., v_n$ von $\mathscr{A}_\theta \mathscr{A}_\theta^*$ gegeben. Da die Berechnung der Hermiteschen Normalform aber nur über einem euklidischen Grundring R effektiv durchfürbar ist, muß man bei einer Implementierung des Verfahrens zusätzlich fordern, daß R euklidisch ist. Um numerische Schwierigkeiten zu vermeiden, empfiehlt es sich einen "Algorithmus modulo D" (siehe [7], § 2.4.2) zu verwenden, etwa eine Variante von [7], Algorithmus 2.4.6. Dazu ist die Kenntnis einer Zahl $D \in R$ erforderlich, die ein Vielfaches von $[R[G]: \mathscr{A}_\theta \mathscr{A}_\theta^*]_R$ ist. In vielen Fällen ist eine Maximalordnung $\mathscr{M}$ mit $R[G] \subseteq \mathscr{A}(X) \subseteq \mathscr{M}$ bekannt und man kann beispielsweise $D = [\mathscr{M} : R[G]]_R$ benutzen.

5. Beispiele

In diesem Abschnitt wollen wir zwei explizite Beispiele berechnen, in denen $G_{L/K}$ jeweils elementar-abelsch von der Ordnung 3^2 ist. Bereits in diesem einfachen Fall fehlen explizite Beschreibungen der assoziierten Ordnungen $\mathscr{A}(K[G_{L/K}]; i)$, $i \in \mathbb{Z}$. In beiden Beispielen liefert der Fall $i = 3$ ein Gegenbeispiel zur Vermutung aus ([4], § 4.3) (siehe auch [5]).

Bei unseren Beispielen handelt es sich um gewisse abelsche Erweiterungen N/M von imaginär-quadratischen Zahlkörpern M, deren Komplettierung nach einem geeigneten Primideal von M die im ersten Teil der Arbeit beschriebene lokale Situation liefert. Wir benutzen hierzu explizite Resultate von R. Schertz ([17], [18]), der für gewisse Strahlklassenerweiterungen von M Potenzganzheitsbasen über dem Hilbertschen Klassenkörper konstruiert hat. Der Vollständigheit halber werden diese Resultate kurz dargestellt. Sei M ein imaginär-quadratischer Zahlkörper, $\mathfrak{f}$ ein ganzes Ideal in M, $M(\mathfrak{f})$ der Strahlklassenkörper modulo $\mathfrak{f}$ über M und $M(1)$ der Hilbertsche Klassenkörper. Wir betrachten nun folgende Normierung der Weierstraßschen $\wp$-Funktion:

Definition 5.1. Für ein ganzes Ideal $\mathfrak{f}$ in M mit der $\mathbb{Z}$-Basis $\mathfrak{f} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\operatorname{Im} \omega_1/\omega_2 > 0$, und $\xi \in K \backslash \mathfrak{f}$ setzt man

$$P(\xi \mid \mathfrak{f}) = \left(\varepsilon \frac{\wp(\xi \mid \mathfrak{f})}{\sqrt[6]{\Delta(\mathfrak{f})}} \right)^e$$

mit einer geeigneten Einheit ε (siehe [17] und [18]) und $e = \frac{1}{2} \# \mu_M$, wobei μ_M die Gruppe der Einheitswurzeln in M bezeichnet. Ferner ist Δ die

Diskriminante aus der Theorie der Modulfunktionen und deren Wurzel wird durch

$$\sqrt[6]{\Delta(\mathfrak{f})} = (2\pi)^2 \eta \left(\frac{\omega_1}{\omega_2}\right)^4 \omega_2^{-2}$$

festgelegt. η bedeutet die Dedekindsche η-Funktion.

Es ist zu bemerken, daß die Werte der P-Funktion durch Auswerten der q-Entwicklungen der Weierstraßschen $\wp$-Funktion ([15], Chapter 4, § 2) und der Dedekindschen η-Funktion ([21] Ch. I, § 4, Prop. 6) auf einfache Weise numerisch zu berechnen sind.

Seien nun $\mathfrak{f}, \mathfrak{g}$ zwei ganze Ideale in M, $\delta \in M$ ein primitiver $\mathfrak{f}$-Teilungspunkt und $\xi \in M$ ein primitiver $\mathfrak{g}$-Teilungspunkt von $\mathbb{C}/\mathfrak{f}\mathfrak{g}$. Setzt man nun

$$\theta = P(\delta \mid \mathfrak{f}\mathfrak{g}) - P(\xi \mid \mathfrak{f}\mathfrak{g}),$$

so erhält man den folgenden

SATZ 5.2. ([17], Satz 4). Ist $\mathfrak{g}$ zusammengesetzt und teilt $\mathfrak{f}$ nicht $2\mathcal{O}_M$, so gilt:

$$\mathcal{O}_{M(\mathfrak{f})} = \mathcal{O}_{M(\mathfrak{g})}[\theta], \qquad \text{falls} \quad \mathfrak{g} \mid \mathfrak{f},$$

$$\mathcal{O}_{M(\mathfrak{f})\,M(\mathfrak{g})} = \mathcal{O}_{M(\mathfrak{g})}[\theta^{-1}], \qquad \text{falls} \quad ggT(\mathfrak{g}, \mathfrak{f}) = 1.$$

Ferner sei darauf hingewiesen, daß die sämtlichen Konjugierten θ^σ, $\sigma \in G_{M(\mathfrak{f})/M(1)}$ von θ bekannt und explizit berechenbar sind (siehe [17], Satz 2). Es wurden nun die folgenden Beispiele betrachtet:

M	p	$\mathfrak{f}$	$\mathfrak{g}$	δ	ξ
$\mathbb{Q}(\sqrt{-1})$	3	(3^2)	$\mathfrak{p}_2\mathfrak{p}_5 = (1+\sqrt{-1})(2+\sqrt{-1})$	$(1+\sqrt{-1})(2+\sqrt{-1})$	9
$\mathbb{Q}(\sqrt{-7})$	3	(3^2)	$\mathfrak{p}_2\overline{\mathfrak{p}_2} = (2)$	2	9

In diesen Fällen ergibt sich $M(\mathfrak{g}) = M(1) = M$ und aus Satz 5.2 folgt daher, daß θ^{-1} eine Potenzganzheitsbasis von $M(\mathfrak{f})$ über M erzeugt. Überdies ist das Primideal $\mathfrak{p} = (p)$ in $M(p^2)/M$ voll verzweigt und θ^{-1} erzeugt das über $\mathfrak{p}$ liegende Primideal von $M(\mathfrak{f})$ (siehe [17], Formel (12) und Satz 3).

Sei nun H die maximale Untergruppe von $G_{M(\mathfrak{f})/M}$ von p-fremder Ordnung und $N = \mathrm{Fix}(H)$. Wir definieren

$$\pi = N_{M(\mathfrak{f})/N}(\theta^{-1}).$$

Damit erzeugt π das über $\mathfrak{p} = (p)$ liegende Primideal von N.

Komplettiert man nun die Erweiterung N/M bezüglich der $\mathfrak{p}$-adischen Bewertung, so erhält man eine lokale Erweiterung L/K.

Sei nun R die Lokalisierung (nicht Komplettierung) von $\mathcal{O}_M$ bezüglich $\mathfrak{p}$. Wir betrachten das Gitter

$$\mathscr{L}_\pi = \left\langle \{\pi^\sigma : \sigma \in G_{N/M}\} \cup \left\{ \frac{1}{p} \operatorname{Sp}_{N/M}(\pi) \right\} \right\rangle_R .$$

LEMMA 5.3. *Für die Komplettierungen der Gitter $\pi^i \mathscr{L}_\pi$, $i \in \mathbb{Z}$, bezüglich $\mathfrak{p}$ gilt*:

$$(\pi^i \mathscr{L}_\pi)_\mathfrak{p} = \mathfrak{p}_L^i .$$

Beweis. Für jedes $\kappa \in L$ mit $v_L(\kappa) = 1$ gilt

$$\mathcal{O}_L = \mathcal{O}_K[G_{L/K}] \left\{ 1, p^{-1} \sum_{g \in G_{L/K}} g \right\} \kappa$$

(siehe [4], Proposition 2.2). Hieraus folgt leicht die Behauptung. ∎

Die Gitter $\pi^i \mathscr{L}_\pi$, $i \in \mathbb{Z}$, sind also $R[G_{N/M}]$-Moduln und es gilt:

$$\mathscr{A}(\pi^i \mathscr{L}_\pi)_\mathfrak{p} = \mathscr{A}(K[G_{L/K}]; i).$$

Zur Berechnung von $\mathscr{A}(\pi^i \mathscr{L}_\pi)$ benötigt man noch die von $\pi^i \mathscr{L}_\pi$ induzierte Darstellung der Galoisgruppe. Sei dazu $\omega_1, ..., \omega_n$ eine R-Basis von $\pi^i \mathscr{L}_\pi$ (etwa $\{\pi^i \pi^\sigma : \sigma \in G_{N/M} \setminus \{1\}\} \cup \{(\pi^i/p) \operatorname{Sp}_{N/M}(\pi)\}$). Zur Berechnung der Darstellungsmatrizen $A(\sigma)$ sind die Koeffizienten a_{ij} folgender Gleichungen

$$\omega_i^\sigma = \sum_{j=1}^n a_{ij} \omega_j, \qquad 1 \leqslant i \leqslant n, \quad \sigma \in G_{N/M},$$

zu bestimmen. Dazu betrachte man das lineare Gleichungssystem

$$\omega_i^{\sigma\tau} = \sum_{j=1}^n a_{ij} \omega_j^\tau, \qquad \tau \in G_{N/M}. \tag{8}$$

Da $\omega_1, ..., \omega_n$ ebenfalls eine Basis von N/M darstellt, ist die Matrix $(\omega_j^\tau)_{1 \leqslant j \leqslant n,\, \tau \in G_{N/M}}$ regulär und (8) ist somit eindeutig lösbar.

Offensichtlich genügt es die assoziierten Ordnungen für $0 \leqslant i < p^2$ zu beschreiben. Ferner kann man die Zahl der zu berechnenden assoziierten Ordnungen durch Dualitätsbetrachtungen weiter reduzieren. Sei dazu

$$\mathfrak{p}_L^{i*} = \{ l \in L \mid \operatorname{Sp}_{L/K}(l \cdot \mathfrak{p}_L^i) \subseteq \mathcal{O}_K \}.$$

Dies ist auf natürliche Weise wieder ein $G_{L/K}$-Modul und es ist leicht nachzurechnen, daß

$$\mathscr{A}(\mathfrak{p}_L^{i}*) = \overline{\mathscr{A}(\mathfrak{p}_L^{i})}$$

gilt, wobei $^-$ den von $\sigma \mapsto \sigma^{-1}$ induzierten Automorphismus von $K[G_{L/K}]$ bedeutet. Ferner berechnet man $\mathscr{D}_{L/K} = \mathfrak{p}_L^{2p^2-2}$ für die Differente von L/K, und somit $\mathfrak{p}_L^{i}* = \mathfrak{p}_L^{-2p^2+2-i}$. Damit erhält man folgende Paarungen dualer Ideale: $(\mathcal{O}_L, \mathfrak{p}_L^2)$, $(\mathfrak{p}_L, \mathfrak{p}_L)$, $(\mathfrak{p}_L^{i}, \mathfrak{p}_L^{p^2+2-i})$, $3 \leqslant i \leqslant p^2-1$.

Außerdem lassen sich in unseren speziellen Beispielen die assoziierten Ordnungen $\mathscr{A}(K[G_{L/K}]; i)$ für $i = 0, 1$ and 5 auf theoretischem Wege explizit berechnen (siehe [5] oder [4], § 4.3). Daher beschränken wir uns bei der Darstellung der numerischen Resultate im Anhang auf die Fälle $i = 3, 4$.

6. Anhang

Im folgenden werden nun die numerischen Werte aufgeführt, die bei der Berechnung der Beispiele aus Abschnitt 5 erhalten wurden. Von besonderem Interesse ist in beiden Beispielen der Fall $i = 3$. Es zeigt sich hier, daß die Vermutung aus ([4], § 4.3) nicht zutrifft (siehe auch [5]). Dieser Fall liefert ebenfalls ein Beispiel für eine Erweiterung $K/\mathbb{Q}_p$, die zwar unverzweigt ist, für die aber dennoch

$$\mathscr{A}(K[G_{L/K}], i) \neq \mathscr{A}(\mathbb{Q}_p[G_{L/K}], i) \otimes_{\mathbb{Z}_p} \mathcal{O}_K$$

für eine ganze Zahl i gilt.

Beispiel 1

Sei zunächst $M = \mathbb{Q}(\sqrt{-1})$. Es sei stets $G_{N/M} = \{\sigma_1, ..., \sigma_9\}$ die Galoisgruppe von N/M. Es ergibt sich folgende Multiplikationstabelle:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9
σ_2	σ_2	σ_3	σ_1	σ_8	σ_7	σ_4	σ_9	σ_6	σ_5
σ_3	σ_3	σ_1	σ_2	σ_6	σ_9	σ_8	σ_5	σ_4	σ_7
σ_4	σ_4	σ_8	σ_6	σ_9	σ_2	σ_7	σ_3	σ_5	σ_1
σ_5	σ_5	σ_7	σ_9	σ_2	σ_6	σ_1	σ_4	σ_3	σ_8
σ_6	σ_6	σ_4	σ_8	σ_7	σ_1	σ_5	σ_2	σ_9	σ_3
σ_7	σ_7	σ_9	σ_5	σ_3	σ_4	σ_2	σ_8	σ_1	σ_6
σ_8	σ_8	σ_6	σ_4	σ_5	σ_3	σ_9	σ_1	σ_7	σ_2
σ_9	σ_9	σ_5	σ_7	σ_1	σ_8	σ_3	σ_6	σ_2	σ_4

Für das Element π und seine Konjugierten erhalten wir:

$$\begin{aligned}
\pi^{\sigma_1} &= -0.027661116582152049162457599058099752858724307530 78 \\
&\quad -0.019171541173769996864279710742417688178082218454 56 * i, \\
\pi^{\sigma_2} &= -0.557934143614055462359614916679401472137998347276 87 \\
&\quad -0.653162979663961763146269849470368473590131944613 23 * i, \\
\pi^{\sigma_3} &= -0.022758048912498182812329073163079077898147537238 93 \\
&\quad +0.224877537475151175153972487132509650656760976666 06 * i, \\
\pi^{\sigma_4} &= 2.092537858247835284548149863673161531320950309931 48 \\
&\quad -0.259991187142933888069885941511530917085409432791 76 * i, \\
\pi^{\sigma_5} &= -8.751878081184899208994826134639850433499591322211 7 \\
&\quad +3.617764422926251169718750990921974878488799674527 15 * i, \\
\pi^{\sigma_6} &= -2.696112702518633721165290724284012797129095381337 26 \\
&\quad +0.586199649151614199846880767392646565560196103612 08 * i, \\
\pi^{\sigma_7} &= -0.549151634584468820160446029506741647564951802694 1 \\
&\quad +0.501680038997122812703151935221603102931460194712 98 * i, \\
\pi^{\sigma_8} &= -2.359788254568677912948626135966368812996406262810 25 \\
&\quad +2.827513503185429543830383438874596089807819159591 9 * i, \\
\pi^{\sigma_9} &= -2.127253876282449926944559250375607537236035346934 71 \\
&\quad +2.171290556215096716827295882180986791108587186622 88 * i.
\end{aligned}$$

Durch Berechnung der elementarsymmetrischen Funktionen erhalten wir das Minimalpolynom über M von π:

$$\begin{aligned}
&x^9 + (15 - 9i)\, x^8 + (36 - 90i)\, x^7 - (90 + 171i)\, x^6 - (171 - 252i)\, x^5 \\
&\quad + (333 + 828i)\, x^4 + (567 + 756i)\, x^3 + (441 + 261i)\, x^2 \\
&\quad + (81 - 36i)\, x + 3.
\end{aligned}$$

Wir berechnen nun mit dem Verfahren aus Abschnitt 4 die assoziierten Ordnungen der Gitter $\pi^i \mathscr{L}_\pi$ für $i = 3, 4$. Hierfür sei $\mathscr{A}(M[G_{N/M}]; \pi^i \mathscr{L}_\pi) = \langle \lambda_1, ..., \lambda_9 \rangle_R$.

Der Fall $i=3$

$$\lambda_1=\sigma_1,\qquad \lambda_2=(801-739*i)\,\sigma_3,\qquad \lambda_3=(739+801*i)\,\sigma_2$$

$$\lambda_4=(-739-801*i)\,\sigma_9,\qquad \lambda_5=(-739-801*i)\,\sigma_6,$$

$$\lambda_6=(-801+739*i)\,\sigma_5,\qquad \lambda_7=(739+801*i)\,\sigma_8,$$

$$\begin{aligned}\lambda_8=&\tfrac{1}{3}(1+1*i)\,\sigma_1+\tfrac{1}{3}(739+801*i)\,\sigma_2+\tfrac{1}{3}(1540+62*i)\,\sigma_3\\&+\tfrac{1}{3}(-1540-62*i)\,\sigma_5+\tfrac{1}{3}(-801+739*i)\,\sigma_6+\tfrac{1}{3}(-739-801*i)\,\sigma_7\\&+\tfrac{1}{3}(801-739*i)\,\sigma_8+\tfrac{1}{3}(62-1540*i)\,\sigma_9\end{aligned}$$

$$\begin{aligned}\lambda_9=&\tfrac{1}{3}(-1+1*i)\,\sigma_1+(-31+770*i)\,\sigma_2+\tfrac{1}{3}(1447+2372*i)\,\sigma_3\\&+\tfrac{1}{3}(-31+770*i)\,\sigma_4+\tfrac{1}{3}(-1509-832*i)\,\sigma_5+\tfrac{1}{3}(-1571+708*i)\,\sigma_6\\&+\tfrac{1}{3}(31-770*i)\,\sigma_7+\tfrac{1}{3}(1509+832*i)\,\sigma_8+\tfrac{1}{3}(1571-708*i)\,\sigma_9.\end{aligned}$$

Um $\mathscr{A}(M[G_{N/M}];\pi^3\mathscr{L}_\pi)$ in schönerer Form anzugeben, benötigen wir weitere Notation. Die 4 Untergruppen von $G_{N/M}$ der Ordnung 3 seien gegeben durch

$$H_1=\{\sigma_1,\sigma_2,\sigma_3\},\qquad H_2=\{\sigma_1,\sigma_4,\sigma_9\},$$
$$H_3=\{\sigma_1,\sigma_5,\sigma_6\},\qquad H_4=\{\sigma_1,\sigma_7,\sigma_8\}.$$

Die zugehörigen Untergruppenidempotente bezeichnen wir mit e_i, $i=1,2,3,4$. Sei weiter $f=\sigma_5-1$. Dann gilt:

$$\lambda=f*(e_1+(1+i)\,e_2)\in\mathscr{A}(M[G_{N/M}];\pi^3\mathscr{L}_\pi).$$

Explizit findet man folgende Darstellung:

$$\begin{aligned}\lambda=\tfrac{1}{1187722}\,&((-791794-395394*i)\,\lambda_1+(801+739*i)\,\lambda_2+(1440-62*i)\,\lambda_3\\&+(801+739*i)\,\lambda\kappa_4+(-801-739*i)\,\lambda_5+(739-801*i)\,\lambda_6\\&+(739-801*i)\,\lambda_7+(801+739*i)\,\lambda_8+(-1478+1602*i)\,\lambda_9).\end{aligned}$$

Damit hat $\mathscr{A}(M[G_{N/M}];\pi^3\mathscr{L}_\pi)$ die folgende Gestalt:

$$\mathscr{A}(M[G_{N/M}];\pi^3\mathscr{L}_\pi)=\langle\sigma\colon\sigma\in G_{N/M},\lambda,pe_G\rangle_R.$$

Der Fall $i=4$

$$\lambda_1=\sigma_1,\qquad \lambda_2=(-739-801*i)\,\sigma_3,\ \lambda_3=(801-739*i)\,\sigma_2,$$
$$\lambda_4=(-739-801*i)\,\sigma_9,\qquad \lambda_5=(739+801*i)\,\sigma_6,$$
$$\lambda_6=(770+31*i)\,\sigma_2+(31-770*i)\,\sigma_3+(-31+770*i)\,\sigma_5$$
$$+(31-770*i)\,\sigma_9,$$
$$\lambda_7=(770+31*i)\,\sigma_2+(-31+770*i)\,\sigma_6+(-770-31*i)\,\sigma_8,$$
$$\lambda_8=(770+31*i)\,\sigma_2+(-770-31*i)\,\sigma_7+(31-770*i)\,\sigma_9,$$
$$\lambda_9=\tfrac{1}{3}(-1+1*i)\,\sigma_1+\tfrac{1}{3}(-1540-62*i)\,\sigma_2+\tfrac{1}{3}(-1540-62*i)\,\sigma_3$$
$$+\tfrac{1}{3}(770+31*i)\,\sigma_4+\tfrac{1}{3}(770+31*i)\,\sigma_5+\tfrac{1}{3}(-1540-62*i)\,\sigma_6$$
$$+\tfrac{1}{3}(770+31*i)\,\sigma_7+\tfrac{1}{3}(770+31*i)\,\sigma_8+\tfrac{1}{3}(-1540-62*i)\,\sigma_9.$$

Es gilt:

$$\mathscr{A}(M[G_{N/M}]\colon \pi^4\mathscr{L}_\pi)=\langle \sigma\colon \sigma\in G_{N/M}, pe_G\rangle_R.$$

Beispiel 2

Sei nun $M=\mathbb{Q}(\sqrt{-7})$ und $\alpha=(1+\sqrt{-7})/2$. Es wurde die folgende Multiplikationstabelle berechnet:

σ_1	σ_2	σ_1	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9
σ_2	σ_2	σ_3	σ_1	σ_7	σ_6	σ_8	σ_9	σ_5	σ_4
σ_3	σ_3	σ_1	σ_2	σ_9	σ_8	σ_5	σ_4	σ_6	σ_7
σ_4	σ_4	σ_7	σ_9	σ_6	σ_3	σ_1	σ_8	σ_2	σ_5
σ_5	σ_5	σ_6	σ_8	σ_3	σ_7	σ_9	σ_1	σ_4	σ_2
σ_6	σ_6	σ_8	σ_5	σ_1	σ_9	σ_4	σ_2	σ_7	σ_3
σ_7	σ_7	σ_9	σ_4	σ_8	σ_1	σ_2	σ_5	σ_3	σ_6
σ_8	σ_8	σ_5	σ_6	σ_2	σ_4	σ_7	σ_3	σ_9	σ_1
σ_9	σ_9	σ_4	σ_7	σ_5	σ_2	σ_3	σ_6	σ_1	σ_8

Für π und seine Konjugierten ergibt sich

$$\pi^{\sigma_1}=-0.20148443333056884289584763338817989642433858227896,$$
$$\pi^{\sigma_2}=-12.25794364480198842360454245004484828876986747569614,$$
$$\pi^{\sigma_3}=-15.60253789426751139165570049189857110638634997244825,$$
$$\pi^{\sigma_4}=1.26073093406634246754368809117585016438305535192933$$
$$-1.01707559110484047688597565548524415869623525911601*i,$$

$$\pi^{\sigma_5} = 1.26073093406634246754368809117585016438305535192936$$
$$+ 1.01707559110484047688597565548524415869623525911601 * i,$$
$$\pi^{\sigma_6} = -0.02895326846113448018411300682779781648598729916795$$
$$+ 0.21044767809174608919883893512493041846560351327044 * i,$$
$$\pi^{\sigma_7} = -0.02895326846113448018411300682779781648598729916794$$
$$- 0.21044767809174608919883893512493041845560351327043 * i,$$
$$\pi^{\sigma_8} = 0.79920532059482634171847020331774729789320996246103$$
$$+ 0.13697627580285178942846077778258405926007975552868 * i,$$
$$\pi^{\sigma_9} = 0.79920532059482634171847020331774729789320996246102$$
$$- 0.13697627580285178942846077778258405926007975555287 * i.$$

Das Element π genügt folgender Minimalgleichung:

$$x^9 + 24x^8 + 90x^7 - 567x^6 + 1089x^5 - 783x^4 + 117x^3 + 36x^2 + 9x + 3.$$

Strukturiell sind die Resultate in diesem Beispiel völlig analog zum ersten Beispiel.

Der Fall $i = 3$

$$\lambda_1 = \sigma_1, \qquad \lambda_2 = 10900\sigma_3, \qquad \lambda_3 = -5450\sigma_2 + 5450\sigma_3,$$
$$\lambda_4 = (10900 - 10900 * \alpha)\,\sigma_6, \qquad \lambda_5 = 10900 * \alpha * \sigma_7,$$
$$\lambda_6 = (-5450 + 5450 * \alpha)\,\sigma_4 + (5450 - 5450 * \alpha)\,\sigma_6,$$
$$\lambda_7 = 5450 * \alpha * \sigma_5 + 5450 * \alpha * \sigma_7,$$
$$\lambda_8 = \tfrac{1}{3}\sigma_1 + \tfrac{1}{3}(2180 - 2180 * \alpha)\,\sigma_2 + \tfrac{1}{3}(-6540 + 15260 * \alpha)\,\sigma_3$$
$$+ \tfrac{1}{3}(6540 - 2180 * \alpha)\,\sigma_4 + \tfrac{1}{3}(-2180 - 2180 * \alpha)\,\sigma_5$$
$$+ \tfrac{1}{3}(-37060 + 8720 * \alpha)\,\sigma_6 + \tfrac{1}{3}(-34880 + 8720 * \alpha)\,\sigma_7 + \tfrac{2180}{3}\sigma_9,$$
$$\lambda_9 = \tfrac{1}{3}(1090 - 2180 * \alpha)\,\sigma_2 + \tfrac{1}{3}(-7630 + 15260 * \alpha)\,\sigma_3$$
$$+ \tfrac{1}{3}(5450 - 2180 * \alpha)\,\sigma_4 + \tfrac{1}{3}(-3270 - 2180 * \alpha)\,\sigma_5$$
$$+ \tfrac{1}{3}(-38150 + 8720 * \alpha)\,\sigma_6 + \tfrac{1}{3}(-35970 + 8720 * \alpha)\,\sigma_7$$
$$+ \tfrac{1}{3}(-35970 + 8720 * \alpha)\,\sigma_7$$
$$- \tfrac{1090}{3}\sigma_8 + \tfrac{1090}{3}\sigma_9.$$

Seien

$$H_1 = \{\sigma_1, \sigma_2, \sigma_3\}, \qquad H_2 = \{\sigma_1, \sigma_4, \sigma_6\},$$
$$H_3 = \{\sigma_1, \sigma_5, \sigma_7\}, \qquad H_2 = \{\sigma_1, \sigma_8, \sigma_9\}.$$

die Untergruppen der Ordnung 3 und $f = \sigma_5 - 1$. Dann gilt:

$$\lambda = f * (e_1 + (1 + 2 * \alpha)\, e_2) \in \mathscr{A}(M[G_{N/M}]; \pi^3 \mathscr{L}_\pi).$$

Explizit hat man die Darstellung

$$\begin{aligned}\lambda = \tfrac{1}{21800}\,&((-14540 - 14540 * \alpha)\,\lambda_1 + (14 - 4 * \alpha)\,\lambda_2 + 8\lambda_3\\ &+ (-12 + 9 * \alpha)\,\lambda_4 + (18 - 6 * \alpha)\,\lambda_5 + (-8 + 8 * \alpha)\,\lambda_6\\ &+ (6 + 2 * \alpha)\,\lambda_7 + (20 + 20 * \alpha)\,\lambda_8 - 20 * \lambda_9).\end{aligned}$$

Es folgt also:

$$\mathscr{A}(M[G_{N/M}]; \pi^3 \mathscr{L}_\pi) = \langle \sigma\colon \sigma \in G_{N/M}, \lambda, pe_G \rangle_R.$$

Der Fall $i = 4$

$$\begin{aligned}&\lambda_1 = \sigma_1, \qquad \lambda_2 = -10900\sigma_3, \qquad \lambda_3 = -10900\sigma_2,\\ &\lambda_4 = (10900 - 10900 * \alpha)\,\sigma_6, \qquad \lambda_5 = 10900 * \alpha * \sigma_7,\\ &\lambda_6 = (-10900 + 10900 * \alpha)\,\sigma_4,\\ &\lambda_7 = -10900 * \alpha * \sigma_5,\\ &\lambda_8 = (-2180 - 4360 * \alpha)\,\sigma_2 + (2180 + 2180 * \alpha)\,\sigma_3\\ &\qquad + (-10900 + 2180 * \alpha)\,\sigma_4 + 4360 * \alpha * \sigma_5\\ &\qquad + (-2180 + 2180 * \alpha)\,\sigma_6 + (4360 + 2180 * \alpha)\,\sigma_7\\ &\qquad - 4360\sigma_9,\\ &\lambda_9 = -\tfrac{1}{3}\sigma_1 + \tfrac{2180}{3}\sigma_2 - \tfrac{4360}{3}\sigma_3 + \tfrac{1}{3}(-17440 - 13080 * \alpha)\,\sigma_4\\ &\qquad + \tfrac{1}{3}(-30520 + 13080 * \alpha)\,\sigma_5 - \tfrac{17440}{3}\sigma_6\\ &\qquad - \tfrac{17440}{3}\sigma_7 - \tfrac{4360}{3}\sigma_8 - \tfrac{4360}{3}\sigma_9.\end{aligned}$$

Hier gilt

$$\mathscr{A}(M[G_{N/M}]; \pi^4 \mathscr{L}_\pi) = \langle \sigma\colon \sigma \in G_{N/M}, pe_G \rangle_R.$$

LITERATUR

1. A. M. BERGÉ, Arithmétique d'une extension à groupe d'inertie cyclique, *Ann. Inst. Fourier* **28** (1978), 17–44.
2. A. M. BERGÉ, A propos du genre de l'anneau des entiers d'une extension, *Publ. Math. Sc. Besançon* (1979–1980), 1–9.
3. Z. I. BOREVICH AND S. V. VOSTOKOV, Rings of integers in an extension of prime degree of a local field as a Galois module, *J. Sov. Math.* **6** (1976), 227–238.
4. D. BURNS, Factorisability and wildly ramified Galois extensions, *Ann. Inst. Fourier* **41** (1991), 393–430.
5. D. BURNS, Eine Bemerkung über arithmetische assoziierte Ordnungen, Universität Augsburg Preprint Nr. 263, 1992.
6. N. P. BYOTT, Some self-dual rings of integers which are not free over their associated orders, *Math. Proc. Cam. Phil. Soc.* **110** (1991), 5–10.
7. H. COHEN, "A Course in Computational Algebraic Number Theory," Springer-Verlag, Berlin/Heidelberg, 1993.
8. M. DEURING, "Algebren," Springer-Verlag, Berlin/New York, 1935.
9. B. EREZ, A survey of recent work on the square root of the inverse different, *Proc. J. Arith. Luminy 1989*, *Astérisque* **198–200** (1991), 133–153.
10. G. G. ELDER AND M. L. MADAN, Galois module structure of integers in wildly ramified $C_p \times C_p$ extensions, preprint, 1994.
11. M. J. FERTON, "Sur l'anneau des entiers d'extensions cycliques de degré p et d'extensions diédrales de degré $2p$ d'un corps local," Thèse de Doctoral de 3e cycle présentée à l'Université de Grenoble, 1972.
12. A. FRÖHLICH, "Galois Module Structure of Algebraic Integers," Springer-Verlag, New York, 1983.
13. A. FRÖHLICH, Module defect and factorisability, *Illinois J. Math.* **32** (1988), 407–421.
14. H. JACOBINSKI, Über die Hauptordnung eines Körpers als Gruppenmodul, *Crelle* **213** (1963), 151–164.
15. S. LANG, "Elliptic Functions," Springer-Verlag, New York/Heidelberg/Berlin, 1987.
16. M. RZEDOWSKI CALDERÓN, G. D. VILLA SALVADOR, AND M. L. MADAN, Galois module structure of rings of integers, *Math. Z.* **204** (1990), 401–424.
17. R. SCHERTZ, Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern, *Crelle* **398** (1989), 105–129.
18. R. SCHERTZ, Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper, *J. Number Theory* **34** (1990), 41–53.
19. J. GRAF V. SCHMETTOW, Kant—a tool for computations in algebraic number fields, *in* "Computational Number Theory" (A. Pethö, M. E. Pohst, H. C. Williams, and H. G. Zimmer, Eds.), pp. 321–330, de Gruyter, 1991.
20. J. P. SERRE, "Corps Locaux," Hermann, Paris, 1962.
21. C. L. SIEGEL, "Lectures on Advanced Analytic Number Theory," Tata Institute of Fundamental Research, Bombay, 1961.
22. M. J. TAYLOR, Formal groups and Galois module structure of local rings of integers, *Crelle* **358** (1985), 97–103.
23. S. V. VOSTOKOV, Ideals of an abelian p-extension of an irregular local field as Galois modules, *J. Sov. Math.* **9** (1978), 299–317.
24. S. V. VOSTOKOV, Ideals of an abelian p-extension of a local field as Galois modules, *J. Sov. Math.* **11** (1979), 567–584.